Cyclic Group: A group G is called a cyclic group if $\exists$ an element $a \in G$, such that every element of G can be expressed as a power of a. In that case a is called generator of G. Notation $G = \langle a \rangle$ or $G = (a) = \{a^n \mid n \in \mathbb{Z}\}$.

Ex. 1. $G = \{1, -1, i, -i\}$ under multiplication is cyclic as
i, $i^2 = i \times i = -1$, $i^3 = i^2 \times i = -i$, $i^4 = 1$.
Thus, i (or $-i$) is a generator of this group.
And order of i is 4 ($\because i^4 = 1$) and order of group G is also 4.

→ If G is cyclic then $o(a) = o(G)$, for some $a \in G$ and conversely. [For finite groups only]

Subgroup: A non empty subset H of a group G is said to be a subgroup of G, if H forms a group under the binary operation of G.

If G is a group with identity element e then the subsets $\{e\}$ and G are trivial subgroups of G. Rest are called non-trivial (or proper) subgroups.

Ex. $(\mathbb{Z}, +)$ is subgroup of $(\mathbb{Q}, +)$, $(\mathbb{Q}, +)$ is subgroup of $(\mathbb{R}, +)$, $(\mathbb{R}, +)$ is subgroup of $(\mathbb{C}, +)$. And these are proper subgroups.

[Two-step test]

Theorem 1: A non empty subset H of a group G is a subgroup of G iff (i) $a, b \in H \Rightarrow ab \in H$ [closure law]

(ii) $a \in H \Rightarrow a^{-1} \in H$. [Inverse law]

Pf:- Let H be a subgroup of G then by definition, (i) & (ii) holds.

Conversely, let (i) & (ii) hold in H. To show H is group.

There are 4 properties of group (Closure, associative, identity & inverse)

Closure holds in H by (i)

Again, $a, b, c \in H \Rightarrow a, b, c \in G \Rightarrow a*(b*c) = (a*b)*c$

So, associativity holds in H

Now, for any $a \in H$, $a^{-1} \in H$ (by ii)

by (i), $aa^{-1} \in H \Rightarrow e \in H$

$\therefore$, H has identity.

Inverse of each element of H is in H by (ii).

Hence, H satisfies all conditions of the definition of group and so it forms a group and therefore H is a subgroup of G.

Theorem 2: A non empty finite subset H of a group G is a subgroup of G iff H holds closure law.

Pf:- If H is a subgroup of G then it is closed under BO of G by definition, so there is nothing to prove.

Conversely, let H be a finite subset which hold closure law

i.e. $a, b \in H \Rightarrow ab \in H$.

Now, to show $a \in H \Rightarrow a^{-1} \in H$.

Since $H \neq \phi$ then there exists an element in H, call it a.

If $a = e$ then $e^{-1} = e \in H$.

If $a \neq e$, then by closure, $a, a^2, a^3, \ldots \in H$.
Since H is finite, for some n, m; $a^n = a^m$, $n > m$

i.e. $a^n a^{-m} = a^m a^{-m} \Rightarrow a^{n-m} = e$, $n-m > 1$ as $a \neq e$.

or, $a^{n-m-1} \cdot a = e$

$\Rightarrow a^{n-m-1}$ is inverse of a and we supposed above that H contains all power of a

$\therefore a^{n-m-1} \in H$ whenever $a \in H$.

Thus, H satisfies both laws (closure, inverse)

Hence, H is subgroup of G.

Theorem 3: In any group G, the powers of any fixed element $a \in G$ constitute a subgroup of G.

Pf:- Consider G' consists of all powers of an element $a \in G$

Closure holds as any two elements of G' has the form a^r & a^s. Then $a^r * a^s = a^{r+s}$. And a^{r+s} is again an element of power of a. So it belongs to G'.

Inverse holds as for any $a^r \in G'$, a^{-r} also belongs to G' as a^{-r} is also power of a.

And $a^r * a^{-r} = e$, that means a^{-r} is inverse of a^r.

Thus, by two-step test, G' is subgroup of G.

Theorem 4: Let G be a finite cyclic group generated by an element $a \in G$. If G is of order n then $a^n = e$, so that $G = \{a, a^2, a^3, \ldots, a^n = e\}$. Moreover n is the least +ve integer for which $a^n = e$.

Pf:- If possible let $a^m = e$ for some positive integer $m < n$.
Since G is generated by a, any element of G can be written as a^k for some integer k. k can be written as $mq + r$ where q is some integer and $0 \leq r < m$. This leads to

$$a^k = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r = e^q * a^r = a^r$$

so that every element of G can be expressed as a^r for some r, $0 \leq r < m$. This means that G has at most m distinct elements and the order of G is $m < n$.
Thus we arrive at a contradiction.
Hence $a^m = e$ for $m < n$ is not possible.